

Approaching Blokh-Zyablov Error Exponent with Linear-Time Encodable/Decodable Codes

Zheng Wang, *Student Member, IEEE*, Jie Luo, *Member, IEEE*

Abstract—Guruswami and Indyk showed in [1] that Forney’s error exponent can be achieved with linear coding complexity over binary symmetric channels. This paper extends this conclusion to general discrete-time memoryless channels and shows that Forney’s and Blokh-Zyablov error exponents can be arbitrarily approached by one-level and multi-level concatenated codes with linear encoding/decoding complexity. The key result is a revision to Forney’s general minimum distance decoding algorithm, which enables a low complexity integration of Guruswami-Indyk’s outer codes into the concatenated coding schemes.

Index Terms—coding complexity, concatenated code, error exponent

I. INTRODUCTION

Consider communication over a discrete-time memoryless channel modeled by a conditional point mass function (PMF) or probability density function (PDF) $p_{Y|X}(y|x)$, where $x \in X$ and $y \in Y$ are the input and output symbols, X and Y are the input and output alphabets, respectively. Let \mathcal{C} be the Shannon capacity. Fano showed in [2] that the minimum error probability P_e for block channel codes of rate R and length N is bounded by

$$\lim_{N \rightarrow \infty} -\frac{\log P_e}{N} \geq E(R), \quad (1)$$

where $E(R)$ is a positive function of channel transition probabilities, known as the error exponent. For finite input and output alphabets, without coding complexity constraint, the maximum achievable $E(R)$ is given by Gallager in [3],

$$E(R) = \max_{p_X} E_L(R, p_X), \quad (2)$$

where p_X is the input distribution, and $E_L(R, p_X)$ is given for different values of R as follows,

$$\begin{aligned} \max_{\rho \geq 1} \{-\rho R + E_x(\rho, p_X)\} & \quad 0 \leq R \leq R_x \\ -R + E_0(1, p_X) & \quad R_x \leq R \leq R_{crit} \\ \max_{0 \leq \rho \leq 1} \{-\rho R + E_0(\rho, p_X)\} & \quad R_{crit} \leq R \leq \mathcal{C}. \end{aligned} \quad (3)$$

The definitions of other variables in (3) can be found in [4]. If we replace the PMF by PDF, the summations by integrals and the max operators by sup in (2), (3), the maximum achievable error exponent for continuous channels, i.e., channels whose input and/or output alphabets are the set of real numbers [3], is still given by (2).

In [4], Forney proposed a one-level concatenated coding scheme, which can achieve the following error exponent, known as Forney’s exponent, for any rate $R < \mathcal{C}$ with a complexity of $O(N^4)$.

$$E_c(R) = \max_{r_o \in [\frac{R}{\mathcal{C}}, 1]} (1 - r_o) E\left(\frac{R}{r_o}\right), \quad (4)$$

where r_o and R are the outer and the overall rates, respectively. Forney’s coding scheme concatenates a maximum distance separable (MDS) outer error-correction code with well performed inner channel codes. To achieve $E_c(R)$, the decoder is required to exploit reliability information from the inner codes using a general minimum distance (GMD) decoding algorithm [4]. Forney’s GMD algorithm essentially carries out outer code decoding, under various conditions, for $O(N)$ times. The overall decoding complexity of $O(N^4)$ is due to the fact that the outer code (which is a Reed-Solomon code) used in [4] has a decoding complexity of $O(N^3)$. Forney’s concatenated codes were generalized to multi-level concatenated codes, also known as the generalized concatenated codes, by Blokh and Zyablov in [5]. As the order of concatenation goes to infinity, the error exponent approaches the following Blokh-Zyablov bound (or Blokh-Zyablov error exponent) [5][6].

$$E^{(\infty)}(R) = \max_{p_X, r_o \in [\frac{R}{\mathcal{C}}, 1]} \left(\frac{R}{r_o} - R \right) \left[\int_0^{\frac{R}{r_o}} \frac{dx}{E_L(x, p_X)} \right]^{-1}. \quad (5)$$

In [1], Guruswami and Indyk proposed a family of linear-time encodable/decodable nearly MDS error-correction codes. By concatenating these codes (as outer codes) with *fixed-lengthed* binary inner codes, together with Justesen’s GMD algorithm [7], Forney’s error exponent was shown to be achievable over binary symmetric channels (BSCs) with a complexity of $O(N)$ [1], i.e., linear in the codeword length. The number of outer code decodings required by Justesen’s GMD algorithm is only a constant¹, as opposed to $O(N)$ in Forney’s case [4]. Since each outer code decoding has a complexity of $O(N)$, upper-bounding the number of outer code decodings by a constant is required for achieving the overall linear complexity. Because Justesen’s GMD algorithm assumes binary channel outputs [7][8], achievability of Forney’s exponent was only proven for BSCs in [1, Theorem 8].

The authors are with the Electrical and Computer Engineering Department, Colorado State University, Fort Collins, CO 80523. E-mail: {zhwang, rocky}@engr.colostate.edu.

¹Strictly speaking, the required number of outer code decodings is linear in the inner codeword length, which is fixed at a reasonably large constant.

In this paper, we show that Forney's GMD algorithm can be revised to carry out outer code decoding for only a constant number of times². With the help of the revised GMD algorithm, by using Guruswami-Indyk's outer codes with fixed-lengthed inner codes, one-level and multi-level concatenated codes can arbitrarily approach Forney's and Blokh-Zyablov exponents with linear complexity, over general discrete-time memoryless channels.

II. REVISED GMD ALGORITHM AND ITS IMPACT ON CONCATENATED CODES

Consider one-level concatenated coding schemes. Assume, for an arbitrarily small $\varepsilon_1 > 0$, we can construct a linear encodable/decodable outer error-correction code, with rate r_o and length N_o , which can correct t symbol errors and d symbol erasures so long as $2t + d < N_o(1 - r_o - \varepsilon_1)$. Note that this is possible for large N_o as shown by Guruswami and Indyk in [1]. To simplify the notations, we assume $N_o(1 - r_o - \varepsilon_1)$ is an integer. The outer code is concatenated with suitable inner codes with rate R_i and fixed length N_i . The rate and length of the concatenated code are $R = r_o R_i$ and $N = N_o N_i$, respectively. In Forney's GMD decoding, inner codes forward not only the estimates $\hat{\mathbf{x}}_m = [\hat{x}_1, \dots, \hat{x}_i, \dots, \hat{x}_{N_o}]$ but also a reliability vector $\boldsymbol{\alpha} = [\alpha_1, \dots, \alpha_i, \dots, \alpha_{N_o}]$ to the outer code, where $\hat{x}_i \in GF(q)$, $0 \leq \alpha_i \leq 1$ and $1 \leq i \leq N_o$. Let

$$s(\hat{x}, x) = \begin{cases} +1 & x = \hat{x} \\ -1 & x \neq \hat{x} \end{cases} \quad (6)$$

For any outer codeword $\mathbf{x}_m = [x_{m1}, x_{m2}, \dots, x_{mN_o}]$, define a dot product $\boldsymbol{\alpha} \cdot \mathbf{x}_m$ as follows

$$\boldsymbol{\alpha} \cdot \mathbf{x}_m = \sum_{i=1}^{N_o} \alpha_i s(\hat{x}_i, x_{mi}) = \sum_{i=1}^{N_o} \alpha_i s_i. \quad (7)$$

Theorem 1: There is at most one codeword \mathbf{x}_m that satisfies

$$\boldsymbol{\alpha} \cdot \mathbf{x}_m > N_o(r_o + \varepsilon_1). \quad (8)$$

Theorem 1 is implied by Theorem 3.1 in [4].

Rearrange the weights in ascending order of their values and let $i_1, \dots, i_j, \dots, i_{N_o}$ be the indices such that

$$\alpha_{i_1} \leq \dots \leq \alpha_{i_j} \leq \dots \leq \alpha_{i_{N_o}}. \quad (9)$$

Define $\mathbf{q}_k = [q_k(\alpha_1), \dots, q_k(\alpha_j), \dots, q_k(\alpha_{N_o})]$, for $0 \leq k < 1/\varepsilon_2$, where $\varepsilon_2 > 0$ is a positive constant with $1/\varepsilon_2$ being an integer, and $q_k(\alpha_{i_j})$ is given by

$$q_k(\alpha_{i_j}) = \begin{cases} 0 & \text{if } \alpha_{i_j} \leq k\varepsilon_2 \\ & \text{and } i_j \leq N_o(1 - r_o - \varepsilon_1) \\ 1 & \text{otherwise} \end{cases} \quad (10)$$

Define dot product $\mathbf{q}_k \cdot \mathbf{x}_m$ as

$$\mathbf{q}_k \cdot \mathbf{x}_m = \sum_{i=1}^{N_o} q_k(\alpha_i) s(\hat{x}_i, x_{mi}) = \sum_{i=1}^{N_o} q_k(\alpha_i) s_i. \quad (11)$$

Then following theorem gives the key result that enables the revision of Forney's GMD decoder.

²The revision can also be regarded as an extension to Justesen's GMD decoding given in [7].

Theorem 2: If $\boldsymbol{\alpha} \cdot \mathbf{x}_m > N_o(\frac{\varepsilon_2}{2} + (r_o + \varepsilon_1)(1 - \frac{\varepsilon_2}{2}))$, then for some $0 \leq k < 1/\varepsilon_2$, $\mathbf{q}_k \cdot \mathbf{x}_m > N_o(r_o + \varepsilon_1)$.

Proof: Define a set of values $c_j = (j - 1/2)\varepsilon_2$ for $1 \leq j \leq 1/\varepsilon_2$ and an integer $p = \lceil \alpha_{i_{N_o(1-r_o-\varepsilon_1)}}/\varepsilon_2 \rceil$, where $1 \leq p \leq 1/\varepsilon_2$.³

Let

$$\begin{aligned} \lambda_0 &= c_1 \\ \lambda_k &= c_{k+1} - c_k, 1 \leq k \leq p-1 \\ \lambda_p &= \alpha_{i_{N_o(1-r_o-\varepsilon_1)+1}} - c_p \\ \lambda_h &= \alpha_{i_{h-p+N_o(1-r_o-\varepsilon_1)+1}} - \alpha_{i_{h-p+N_o(1-r_o-\varepsilon_1)}}, \\ &\quad \text{if } p < h < p + N_o(r_o + \varepsilon_1) \\ \lambda_{p+N_o(r_o+\varepsilon_1)} &= 1 - \alpha_{i_{N_o}}. \end{aligned} \quad (12)$$

We have

$$\sum_{k=0}^{j-1} \lambda_k = \begin{cases} c_j & 1 \leq j \leq p \\ \alpha_{i_{j-p+N_o(1-r_o-\varepsilon_1)}} & p < j \leq p + N_o(r_o + \varepsilon_1) \end{cases}, \quad (13)$$

and

$$\sum_{k=0}^{p+N_o(r_o+\varepsilon_1)} \lambda_k = 1. \quad (14)$$

Define a new weight vector $\tilde{\boldsymbol{\alpha}} = [\tilde{\alpha}_1, \dots, \tilde{\alpha}_i, \dots, \tilde{\alpha}_{N_o}]$ with

$$\tilde{\alpha}_i = \begin{cases} \operatorname{argmin}_{c_j, 1 \leq j \leq p} |c_j - \alpha_i| & \alpha_i \leq \alpha_{i_{N_o(1-r_o-\varepsilon_1)}} \\ \alpha_i & \alpha_i > \alpha_{i_{N_o(1-r_o-\varepsilon_1)}} \end{cases}. \quad (15)$$

Define $\mathbf{p}_k = [p_k(\alpha_1), \dots, p_k(\alpha_i), \dots, p_k(\alpha_{N_o})]$ with $1 \leq k \leq p + N_o(r_o + \varepsilon_1)$ such that for $0 \leq k < p$

$$\mathbf{p}_k = \mathbf{q}_k, \quad (16)$$

and for $p \leq k \leq p + N_o(r_o + \varepsilon_1)$

$$p_k(\alpha_i) = \begin{cases} 0 & \alpha_i \leq \alpha_{i_{k-p+N_o(1-r_o-\varepsilon_1)}} \\ 1 & \alpha_i > \alpha_{i_{k-p+N_o(1-r_o-\varepsilon_1)}} \end{cases}. \quad (17)$$

We have

$$\tilde{\boldsymbol{\alpha}} = \sum_{k=0}^{p+N_o(r_o+\varepsilon_1)} \lambda_k \mathbf{p}_k. \quad (18)$$

Define a set of indices

$$\mathcal{U} = \{i_1, i_2, \dots, i_{N_o(1-r_o-\varepsilon_1)}\}. \quad (19)$$

According to the definition of $\tilde{\alpha}_i$, for $i \notin \mathcal{U}$, $\tilde{\alpha}_i = \alpha_i$. Hence

$$\tilde{\boldsymbol{\alpha}} \cdot \mathbf{x}_m = \boldsymbol{\alpha} \cdot \mathbf{x}_m + \sum_{i \in \mathcal{U}} (\tilde{\alpha}_i - \alpha_i) s_i. \quad (20)$$

Since $|\tilde{\alpha}_i - \alpha_i| \leq \varepsilon_2/2$, and $s_i = \pm 1$, we have

$$\sum_{i \in \mathcal{U}} (\tilde{\alpha}_i - \alpha_i) s_i \geq -N_o(1 - r_o - \varepsilon_1) \frac{\varepsilon_2}{2}. \quad (21)$$

³Note that the value of p cannot be 0. Because if $p = 0$, i.e., $\alpha_{i_{N_o(1-r_o-\varepsilon_1)}} = 0$, then there are at least $N_o(1 - r_o - \varepsilon_1)$ zeros in vector $\boldsymbol{\alpha}$. Consequently, $\boldsymbol{\alpha} \cdot \mathbf{x}_m \leq N_o(r_o + \varepsilon_1) < N_o(\frac{\varepsilon_2}{2} + (r_o + \varepsilon_1)(1 - \frac{\varepsilon_2}{2}))$, which contradicts the assumption that $\boldsymbol{\alpha} \cdot \mathbf{x}_m > N_o(\frac{\varepsilon_2}{2} + (r_o + \varepsilon_1)(1 - \frac{\varepsilon_2}{2}))$.

Consequently, $\alpha \cdot \mathbf{x}_m > N_o \left(\frac{\varepsilon_2}{2} + (r_o + \varepsilon_1) \left(1 - \frac{\varepsilon_2}{2} \right) \right)$ implies

$$\tilde{\alpha} \cdot \mathbf{x}_m > N_o(r_o + \varepsilon_1). \quad (22)$$

If $\mathbf{p}_k \cdot \mathbf{x}_m \leq N_o(r_o + \varepsilon_1)$ for all \mathbf{p}_k 's, then

$$\begin{aligned} \tilde{\alpha} \cdot \mathbf{x}_m &= \sum_{k=0}^{p+N_o(r_o+\varepsilon_1)} \lambda_k \mathbf{p}_k \cdot \mathbf{x}_m \\ &\leq N_o(r_o + \varepsilon_1) \sum_{k=0}^{p+N_o(r_o+\varepsilon_1)} \lambda_k \\ &= N_o(r_o + \varepsilon_1), \end{aligned} \quad (23)$$

which contradicts (22). Therefore, there must be some \mathbf{p}_k that satisfies

$$\mathbf{p}_k \cdot \mathbf{x}_m > N_o(r_o + \varepsilon_1). \quad (24)$$

Since for $k \geq p$, \mathbf{p}_k has no more than $N_o(r_o + \varepsilon_1)$ number of 1's, which implies $\mathbf{p}_k \cdot \mathbf{x}_m \leq N_o(r_o + \varepsilon_1)$, the vectors that satisfy (24) must exist among \mathbf{p}_k with $1 \leq k < p$. In words, for some k , $\mathbf{q}_k \cdot \mathbf{x}_m > N_o(r_o + \varepsilon_1)$. ■

Theorems 1 and 2 indicate that, if \mathbf{x}_m is transmitted and $\alpha \cdot \mathbf{x}_m > N_o \left(\frac{\varepsilon_2}{2} + (r_o + \varepsilon_1) \left(1 - \frac{\varepsilon_2}{2} \right) \right)$, for some $0 \leq k < 1/\varepsilon_2$, errors-and-erasures decoding specified by \mathbf{q}_k (where symbols with $\mathbf{q}_k(\alpha_i) = 0$ are erased) will output \mathbf{x}_m . Since the total number of \mathbf{q}_k vectors is upper bounded by a constant $1/\varepsilon_2$, the outer code carries out errors-and-erasures decoding only for a constant number of times. Consequently, a GMD decoding that carries out errors-and-erasures decoding for all \mathbf{q}_k 's and compares their decoding outputs can recover \mathbf{x}_m with a complexity of $O(N_o)$. Since the inner code length N_i is fixed, the overall complexity is $O(N)$.

The following theorem gives an error probability bound for one-level concatenated codes with the revised GMD decoder.

Theorem 3: Assume inner codes achieve Gallager's error exponent given in (2). Let the reliability vector α be generated according to Forney's algorithm presented in [4, Section 4.2]. Let \mathbf{x}_m be the transmitted outer codeword. For large enough N , error probability of the one-level concatenated codes is upper bounded by

$$\begin{aligned} P_e &\leq P \left\{ \alpha \cdot \mathbf{x}_m \leq N_o \left(\frac{\varepsilon_2}{2} + (r_o + \varepsilon_1) \left(1 - \frac{\varepsilon_2}{2} \right) \right) \right\} \\ &\leq \exp [-N (E_c(R) - \varepsilon)], \end{aligned} \quad (25)$$

where $E_c(R)$ is Forney's error exponent given by (4) and ε is a function of ε_1 and ε_2 with $\varepsilon \rightarrow 0$ if $\varepsilon_1, \varepsilon_2 \rightarrow 0$.

The proof of Theorem 3 can be obtained by first replacing Theorem 3.2 in [4] with Theorem 2, and then following Forney's analysis presented in [4, Section 4.2].

The difference between Forney's and the revised GMD decoding schemes lies in the definition of errors-and-erasures decodable vectors \mathbf{q}_k , the number of which determines the decoding complexity. Forney's GMD decoding needs to carry out errors-and-erasures decoding for a number of times linear in N_o , whereas ours for a constant number of times. Although the idea behind the revised GMD decoding is similar to Justesen's GMD algorithm

[7], Justesen's work has focused on error-correction codes where inner codes forward Hamming distance information (in the form of an α vector) to the outer code.

Applying the revised GMD algorithm to multi-level concatenated codes [5][6] is quite straightforward. Achievable error exponent of an m -level concatenated codes is given in the following Theorem.

Theorem 4: For a discrete-time memoryless channel with capacity \mathcal{C} , for any $\varepsilon > 0$ and any integer $m > 0$, one can construct a sequence of m -level concatenated codes whose encoding/decoding complexity is linear in N , and whose error probability is bounded by

$$\begin{aligned} \lim_{N \rightarrow \infty} -\frac{\log P_e}{N} &\geq E^{(m)}(R) - \varepsilon, \\ E^{(m)}(R) &= \max_{p_X, r_o \in [\frac{\mathcal{C}}{2}, 1]} \frac{\frac{R}{r_o} - R}{\frac{R}{r_o m} \sum_{i=1}^m \left[E_L \left(\left(\frac{i}{m} \right) \frac{R}{r_o}, p_X \right) \right]^{-1}} \end{aligned} \quad (26)$$

The proof of Theorem 4 can be obtained by combining Theorem 3 and the derivation of $E^{(m)}(R)$ in [5][6].

Note that $\lim_{m \rightarrow \infty} E^{(m)}(R) = E^{(\infty)}(R)$, where $E^{(\infty)}(R)$ is the Blokh-Zyablov error exponent given in (5). Theorem 4 implies that, for discrete-time memoryless channels, Blokh-Zyablov error exponent can be arbitrarily approached with linear encoding/decoding complexity.

III. CONCLUSIONS

We proposed a revised GMD decoding algorithm for concatenated codes over general discrete-time memoryless channels. By combining the GMD algorithm with Guruswami and Indyk's error correction codes, we showed that Forney's and Blokh-Zyablov error exponents can be arbitrarily approached by one-level and multi-level concatenated coding schemes, respectively, with linear encoding/decoding complexity.

ACKNOWLEDGMENT

The authors would like to thank Professor Alexander Barg for his help on multi-level concatenated codes.

REFERENCES

- [1] V. Guruswami and P. Indyk, "Linear-Time Encodable/Decodable Codes With Near-Optimal Rate," *IEEE Trans. Inform. Theory*, Vol. 51, No. 10, pp. 3393-3400, Oct. 2005.
- [2] R. Fano, "Transmission of Information," *The M.I.T Press, and John Wiley & Sons, Inc.*, New York, N.Y., 1961.
- [3] R. Gallager, "A Simple Derivation of The Coding Theorem and Some Applications," *IEEE Trans. on Inform. Theory*, Vol.11, pp.3-18, Jan. 1965.
- [4] G. Forney, "Concatenated Codes," *The MIT Press*, 1966.
- [5] E. Blokh and V. Zyablov, "Linear Concatenated Codes," Nauka, Moscow, 1982 (In Russian).
- [6] A. Barg and G. Zemor, "Concatenated Codes: Serial and Parallel," *IEEE Trans. Inform. Theory*, Vol. 51, pp. 1625-1634, May 2005.
- [7] J. Justesen, "A Class of Constructive Asymptotically Good Algebraic Codes," *IEEE Trans. Inform. Theory*, Vol. IT-18, pp. 652-656, Sep. 1972.
- [8] V. Guruswami, "List Decoding of Error-correcting Codes," Ph.D. dissertation, MIT, Cambridge, MA, 2001.